REMARKS/ARGUMENTS

Amendments were made to the specification to correct errors and to clarify the specification. No new matter has been added by any of the amendments to the specification.

Claims 1-21 are pending in the present application. By this response, claims 5-6, 12-13, and 19-20 are amended. Reconsideration of the claims is respectfully requested.

I. Objection to Claims: 5-6, 12-13, and 19-20

The examiner has stated that claims 5-6, 12-13, and 19-20 were objected to for informalities. In response, the claims have been rewritten to overcome this objection.

II. Objection to Specification

The examiner has stated that the specification is objected to for informalities. In response, the specification has been amended to overcome this objection.

III. 35 U.S.C. § 102, Anticipation: Claims 1-4, 8-11, and 15-18

The examiner has rejected claims 1-4, 8-11, and 15-18 under 35 U.S.C. § 102 as being anticipated by *Drake et al.*, Event Detection, U.S. Patent No. 6,347,374 (February 12, 2002) (hereinafter "*Drake*"). This rejection is respectfully traversed. The examiner states:

> As per claim 1, 8, and 15, Drake teaches a method in a data processing system for reporting security situations, comprising the steps of:
>
> logging events by storing event attributes as an event set, wherein each event set includes a source attribute, a target attribute and an event category attribute (Drake: Column 12 Line 43-45 and Column 15 Line 60-67);
>
> classifying events as groups by aggregating events with at least one attribute within the event set as an identical value (Drake: Column 12 Line 2-4, Column 12 Line 38-41 and Column 16 Line 1-8, Column 11 Line 38-50 and Column 14 Line 18-21: Drake teaches aggregating the correlated raw events into event groups with at least one attribute within the event set as an identical value such as (a) same user ID, or (b) same group type as "authentication failure" to generate an alert of severity situations).
>
> calculating severity levels for the groups, wherein a severity level for a group is a function of a number of events comprising the group and values of common elements in the group (Drake: Column 12 L1ne29-30, Column 16 Line 15-18, Column 11 Line38 -50, Column 16 Line 15-18 and Column 14 Line 18-21: the "authentication failure' is qualified to meet the severity level as an event caused by the failures of a user login).
>
> reporting a group from the groups to a user as a situation, if a severity level of the group exceeds a threshold value (Drake: Column 11 Line 38-50 and

> Column 14 Line 18-21: the 'authentication failure" is qualified to meet the severity level as an event caused by the failures of a user login when the aggregating events exceed the predetermined number (i.e., threshold = 3) as taught by Drake).

Office Action dated May 23, 2006, pages 3-4.

A prior art reference anticipates the claimed invention under 35 U.S.C. § 102 only if every element of a claimed invention is identically shown in that single reference, arranged as they are in the claims. *In re Bond*, 910 F.2d 831, 832, 15 U.S.P.Q.2d 1566, 1567 (Fed. Cir. 1990). All limitations of the claimed invention must be considered when determining patentability. *In re Lowry*, 32 F.3d 1579, 1582, 32 U.S.P.Q.2d 1031, 1034 (Fed. Cir. 1994). Anticipation focuses on whether a claim reads on the product or process a prior art reference discloses, not on what the reference broadly teaches. *Kalman v. Kimberly-Clark Corp.*, 713 F.2d 760, 218 U.S.P.Q. 781 (Fed. Cir. 1983). In this case each and every feature of the presently claimed invention is not identically shown in the cited reference, arranged as they are in the claims.

Applicants first address the rejection of claim 1, which is representative of independent claims 8 and 15 with regard to similarly recited subject matter. *Drake* does not anticipate claim 1 because *Drake* does not teach all of the features of claim 1. Claim 1 is as follows:

> 1. A method in a data processing system for reporting security situations, comprising the steps of:
>
> logging events by storing event attributes as an event set, wherein each event set includes a source attribute, a target attribute and an event category attribute;
>
> classifying events as groups by aggregating events with at least one attribute within the event set as an identical value;
>
> calculating severity levels for the groups, wherein a severity level for a group is a function of a number of events comprising the group and values of common elements in the group; and
>
> reporting a group from the groups to a user as a situation, if a severity level of the group exceeds a threshold value.

The examiner states that the feature, "logging events by storing event attributes as an event set, wherein each event set includes a source attribute, a target attribute and an event category attribute" is taught by the following passages of *Drake*:

> The event detection system uses database table relationships to store events and to map event instance data to meta-data.

Drake, column 12, lines 43-45.

> Statistical processors are used to process the following Event detection system features: collect statistical data by category, user, and platform; and analyze statistical data and detect events based on statistical profiles.

> Implementation of statistical processing in the event detection system 10 requires design and implementation of two components. The first is a design of a database schema to permit the storage of statistical data by the following key parameters: event category; user; platform; and interval.

Drake, column 15, lines 60-67.

Drake does not anticipate claim 1 because *Drake* does not teach the above recited feature of claim 1. Specifically, *Drake* does not teach storing event attributes as an event set. "The identical invention must be shown in as complete detail as is contained in the ... claim." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). *Drake* specifically states that a database table is used to store events. Contrary to the examiner's assumptions, storing events in a database table is not the same as grouping event attributes into an event set.

Furthermore, *arguendo*, even if *Drake* teaches an event set, *Drake* does not teach an event set that includes 1) a source attribute, 2) a target attribute, and 3) an event category attribute. *Drake* collects data by 1) category, 2) user, and 3) platform. (*Drake*, column 15, lines 60-67). *Drake*'s user attribute identifies the user performing illegal actions. (*Drake*, column 2, lines 35-40). Assuming that this attribute teaches the source attribute as recited in claim 1, *Drake* does not teach an event set that includes the target attribute. *Drake* teaches a platform attribute. *Drake* does not specifically define the term platform. The meaning of a platform to a person having ordinary skill in the art describes some sort of framework, either in hardware or software, which allows software to run. (*Wikipedia*). An example of a platform would be Windows NT. (*Drake*, column 8, lines 33-34). The target attribute as recited in claim 1 identifies the destination of the attack, i.e. the target computer(s). (*Specification*, page 11, lines 5-11). *Drake*'s platform attribute is clearly not the same as the target attribute of the presently claimed invention. Because *Drake* does not teach or suggest an event set that includes the target attribute, *Drake* does not teach or suggest the above recited feature of claim 1.

Furthermore, *Drake* does not teach the feature "calculating severity levels for the groups, wherein a severity level for a group is a function of a number of events comprising the group and values of common elements in the group" as recited by claim 1. The examiner asserts otherwise, citing to the following passages of *Drake*:

> Information such as the event detection system event number and severity level are derived by this method. At any stage of event processing, meta-data may be derived.

Drake, column 12, lines 29-30.

> The detector 32 counts events as they arrive to see if one of the thresholds is exceeded. If a threshold is exceeded, a high severity event is generated and passed to the inserter 22 for storage in a Virtual Record in the database 12.

Drake, column 16, lines 15-18.

In the present embodiment, there are six, standard, defined severity levels, one of which is assigned to each Virtual Record.

Level	Meaning
0	Irrelevant or undefined
1	Potentially significant event
2	Interesting event
3	Significant event
4	Warning
5	Alert

Drake, column 11, lines 38-50.

For example, consider a set of rules that generates an alert on three failed logins. The rules for this alert are "three failed logins, by a user, at a platform, without an intervening successful login or system restart".

Drake, column 14, lines 18-21.

The first passage above discloses that a rules-based processing method applied to an event record when the record is inserted into the database is used to derive an event detection system event number and severity level. The second passage discloses counting the event to see if one of the thresholds is exceeded. The third passage discloses the various severity levels, such as irrelevant, potentially significant, interesting, significant, warning, and alert, and that each record is assigned one of the severity levels. And the fourth passage discloses a rules-based alert which generates an alert based on three failed logins by a user.

However, the passages above do not teach calculating severity levels for the groups, wherein a severity level for a group is a function of a number of events comprising the group and values of common elements in the group. The passages merely disclose the use of assigning a severity level to a record, and that the rules-based alert may be used to generate an alert upon the failure of a user's 3rd login attempt. There is no discussion in *Drake* of calculating a severity level for a group of events as recited in the claimed invention. The examiner alleges that "authentication failure" is qualified to meet the severity level as an event by the failures of a user login. However, determining whether an alert should be generated based on multiple unsuccessful logins is not the same as calculating a severity level for a group of events. Rather, as shown above in column 11, lines 38-50 and column 12, lines 29-30, *Drake* does not teach assigning severity levels to groups of events, but rather *Drake* explicitly teaches that one severity level is assigned to each Virtual Record. As disclosed in column 6, lines 6-8, *Drake* teaches that a Virtual Record is a "standardized flat representation of an event in a normalized format". Thus, even though *Drake* derives security levels, these levels are derived for each Virtual Record, which represent a single event, rather than a group of events as recited in claim 1. *Drake* does not mention that there is a severity

level calculated for the group itself. Instead, *Drake* discloses an alert is generated if a specific number of the same event occurs (e.g., 3 failed logins by a particular user).

Furthermore, the passages above also do not teach that the severity level for a group is a function of a number of events comprising the group and values of common elements in the group. Thus, the common elements in the group have values which are used to calculate the severity level of the group. *Drake* does not mention a severity level calculated for the group itself and that the severity level of the calculated group is based on common elements in the group. *Drake* merely discloses that an alert is generated based on the occurrence of a specific number of events (e.g., 3 failed logins). Thus, while *Drake* may derive and assign severity levels to individual records in the database tables, *Drake* does not teach anything about calculating a severity level for a group of events, nor does *Drake* teach or suggest that the calculated group severity level is based on a number of events comprising the group and values of common elements in the group.

Because *Drake* does not disclose all the features as recited in claim 1, *Drake* does not anticipate claim 1. For the same reasoning, *Drake* does not anticipate independent claims 8 and 15. At least by virtue of their dependency on claims 1, 8, and 15, respectively, *Drake* also do not teach the features in dependent claims 2-4, 9-11, and 16-18.

Furthermore, claims 2-4, 9-11, and 16-18 recite additional subject matter not taught by *Drake*. For instance, claims 2, 9, and 16 recite that severity levels are calculated based on at least one of the number of event sets within each of the groups, the source attribute of the event sets within each of the groups, the target attribute of the event sets within each of the groups, and the event category attribute of the event sets within each of the groups. As discussed in the response to the rejection of claims 1, 8, and 15 above, the features of calculating severity levels for an event group in these claims are neither taught nor suggested by *Drake*. Furthermore, an event group containing a target attribute is neither taught nor suggested by *Drake*. Consequently, it is respectfully urged that the rejection of claims 1-4, 8-11, and 15-18 under 35 U.S.C. § 102 have been overcome.

IV. 35 U.S.C. § 103, Obviousness: Claims 5-7, 12-14, and 19-21

The examiner has rejected claims 5-7, 12-14, and 19-21 under 35 U.S.C. § 103 as being unpatentable over *Drake* in view of *Burrows et al.*, Method and System for Limiting the Impact of Undesirable Behavior of Computers on a Shared Data Network, U.S. Patent Publication No. 2002/0073338 (June 13, 2002) (hereinafter "*Burrows*"). This rejection is respectfully traversed. The examiner states:

> As per claim 5, 12 and 19, Drake does not disclose expressly the target attribute represents one of a computer and a collection of computers. Burrows teaches the target

attribute represents one of a computer and a collection of computers (Burrows: Para [0050] and Para [0046] Line 10-11: the target attribute could be the single server computer that causes denial-of-service or a collection of computers such as broadcast storms).

As per claim 7, 14 and 21, Drake does not disclose expressly aggregating a subset of the groups into a combined group.

Burrows teaches aggregating a subset of the groups into a combined group (Burrows: Para [0050] and Para [0046] Line 10-11: similar to the Figure 8 / Element 804/806/802 of the instant application, the single source computer that causes broadcast storms to any of the unspecified destination computers, as taught by Burrows, does indeed generate a combined group of events. Likewise, it applies to the similar situation of denial-of-service attacks).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Burrows within the system of Drake because (a) Drake teaches improving network security by providing an effective event detecting systems (Drake, see example, Column 2 Line 4-8 and Column 3 Line 34-35]) and (b) Burrows teaches managing and tracking computer security incidents that may occur in a network computer system by effectively detecting any types of behavior and undesirable patterns of packet traffic (Burrows: Para [0019]).

Office Action dated May 23, 2006, page 6.

Regarding claims 5-7, 12-14, and 19-21, the examiner has failed to state a *prima facie* obviousness rejection because the proposed combination does not teach or suggest all of the features of claims 5-7, 12-14, and 19-21. A *prima facie* case of obviousness is established when the teachings of the prior art itself suggest the claimed subject matter to a person of ordinary skill in the art. *In re Bell*, 991 F.2d 781, 783, 26 U.S.P.Q.2d 1529, 1531 (Fed. Cir. 1993). All limitations of the claimed invention must be considered when determining patentability. *In re Lowry*, 32 F.3d 1579, 1582, 32 U.S.P.Q.2d 1031, 1034 (Fed. Cir. 1994). If an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious. *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988). In the case at hand, not all of the features of the claimed invention have been properly considered and the teachings of the references themselves do not teach or suggest the claimed subject matter to a person of ordinary skill in the art.

Addressing the rejection of claims 5-7, 12-14, and 19-21, the examiner has failed to state a *prima facie* obviousness rejection because neither *Drake* nor *Burrows* teach or suggest all features of claim 1, 8, and 15 from which claims 5-7, 12-14, and 19-21 depend from, respectively. As discussed above, *Drake* does not teach the claimed feature of logging events by storing event attributes as an event set, wherein each event set includes a source attribute, a target attribute and an event category attribute. Because *Drake* specifically teaches collecting data by 1) category, 2) user, and 3) platform, *Drake* also does not suggest the features of claim 1 wherein the event set includes a target attribute. Furthermore, *Burrows*

does not teach or suggest all of the features of claim 1. *Burrows* is directed to detecting undesirable behavior in a network system. Specifically, *Burrows* envisions using a packet traffic monitor to determine the existence and source of any pattern of undesirable behavior. (*Burrows*, paragraph 40). However, *Burrows* does not teach or suggest logging events by "storing event attributes as an event set, wherein each event set includes a source attribute, a target attribute and an event category attribute."

Because neither *Drake* nor *Burrows* teach or suggest all of the features of claim 1, 8, and 15 and because claims 5-7, 12-14, and 19-21 depend from claims 1, 8, and 15, respectively, the proposed combination of *Drake* and *Burrows* when considered as a whole does not teach or suggest all of the features of claims 5-7, 12-14, and 19-21. Accordingly, the examiner has failed to state a *prima facie* obviousness rejection of claims 5-7, 12-14, and 19-21.

Furthermore, the proposed combination of *Drake* nor *Burrows*, when considered as a whole, also does not teach or suggest all of the additional features of claims 5-7, 12-14, and 19-21. For instance, claims 7, 14, and 21 recite "aggregating a subset of the event groups into a combined group." The examiner points to the following passages in *Burrows* as teaching this feature:

> In one embodiment, the packet traffic monitor observes the network and thereby detects and localizes all broadcast packets traffic. Observing more than a predetermined number of broadcast packets within a predetermined time period implies that a broadcast storm is underway. It is likely that the packet is correctly addressed, and that knowing the source MAC address and the network topology will point to a particular port of a forwarding device, e.g., switch port, to be disabled. In another embodiment, the per-port broadcast ingress packet counters can be used to trace broadcast packets to their source. This approach is used if the packet traffic monitor fails at determining the source, possibly because of incorrectly formatted packets or because the misbehaving host has not been seen on the network before (unknown MAC address). This detection approach is less timely than the prior approach since the process of retrieving these counters from the switch is extensive and it cannot be executed often.

Burrows, para [0050].

> For example, the monitor can detect too many packets destined to an overloaded server, too many probe packets directed to a firewall or too many ARP request packets.

Burrows, para [0046], line 10-11.

The cited passages of *Burrows* does not mention aggregating a subset of an event group into a combined event group, as recited in claims 7, 14, and 21. The first passage discusses determining the source of a broadcast storm. A broadcast storm occurs when a host emits a continuous stream of broadcast packets. The second passage merely states that the monitor can detect too many packets

destined to an overloaded server. Neither passage teaches or suggests aggregating a subset of an event group into a combined event group, as recited in claims 7, 14, and 21.

Even if the missing elements of the rejected claims existed in the prior art, for the rejected claims to be obvious there must be some motivation or incentive from the prior art to modify or combine the reference teachings to achieve the present invention. The examiner does not provide any motivation from either reference that making all the necessary modifications to the reference teachings to achieve the present invention would be desirable. If the examiner cannot make such a showing, then the examiner has simply relied on hindsight with the benefit of applicants' disclosure to develop an incentive for the changes, which in fact, would not be obvious to one of ordinary skill in the art at the time the invention was made. Therefore, the rejection of claims 5-7, 12-14, and 19-21 under 35 U.S.C. § 103 has been overcome.

V. Conclusion

It is respectfully urged that the subject application is patentable over the cited references and is now in condition for allowance. The examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

DATE: August 14, 2006

Respectfully submitted,

/Cathrine K. Kinslow/

Cathrine K. Kinslow
Reg. No. 51,886
Yee & Associates, P.C.
P.O. Box 802333
Dallas, TX 75380
(972) 385-8777
Attorney for Applicants

CKK/nhh